Homeland Security Affairs

Volume I, Issue 2 2005 *Article 3*

2005

Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment

Robert B. Watts*

*NPS monterey, rbwatts27@hotmail.com

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Homeland Defense and Security,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment

Robert B. Watts

Abstract

As a maritime nation, the United States is economically and strategically reliant on its ports, a fact well known to our potential enemies in the Global War on Terror. A successful attack against maritime critical infrastructure in our ports has the potential to cause major economic disruption and create mass casualties and conflagration. The United States has faced military threats in its littoral before, and lessons from the past offer value in determining how to defend ports in the modern era. But these lessons must be considered in light of the new asymmetric terrorist threat. By examining lessons from the past and considering current maritime multi-agency capabilities, a logical command and control solution can be devised to effectively fuse agency efforts in tactical defense of maritime critical infrastructure.

AUTHOR BIOGRAPHY: A 1985 graduate of the U.S. Coast Guard Academy, CDR Bob Watts has served six tours at sea, most recently commanding USCGC STEADFAST (WMEC 623) on homeland security duty. A qualified Surface Warfare Officer, he holds post graduate degrees from the Naval War College (CCE), Old Dominion University (History), and American Military University (International Naval Studies). He has been published numerous times in USNI PROCEEDINGS on Coast Guard-Navy strategic issues, including winning the 1998 USNI Colin Powell Joint Essay Contest. He is currently assigned as Coast Guard Liaison Officer to office of the CNO (N5), and is a student in the Naval Post Graduate School's HLS/HLD program.

Throughout its history, the United States has been a global maritime nation, dependent upon the oceans for economy, welfare, and defense. In the modern era emphasis on globalization and the world economy has increased this dependence considerably. There are some 95,000 miles of United States' coastline and 3.4 million square miles of territorial seas and exclusive economic zones in the U.S. maritime domain.[1] Connecting the continental United States to this zone are over 1,000 harbors and ports, 361 of which are cargo capable. Through these ports enter approximately 21,000 containers daily, representing ninety-five percent of the nation's overseas cargo, including 100 percent of U.S. petroleum imports.[2] In addition to commerce, there are seventy-six million recreational boaters in the United States. Six million cruise ship passengers visit U.S. ports annually. In the strategic/military sense, a substantial portion of U.S. national power relies on the sea, both in the form of traditional Navy Carrier Strike groups that deploy from ports in the continental United States and the subsequent ability to reinforce deployed forces overseas. Without unimpeded access to the sea, the ability of the United States to project national power is extremely limited.

Maritime infrastructure is crucial in maintaining this link to the sea. From naval bases to commercial ports, maritime infrastructure is well developed nationwide and is crucial to both the economic sector and military strategy. Maritime infrastructure is critical to the employment of national maritime power and as such is a logical (if not desirable) target for acts of terrorism by our enemies. A successful attack against a port could incur serious economic and military damage, present an enemy with the opportunity to inflict mass casualties, and have serious long-term detrimental effects on our national economy.

Maritime Critical Infrastructure Protection (MCIP) presents many challenges in an asymmetric environment. Previous models of maritime defense have focused on protecting ships from traditional naval attack; even when ports and supporting infrastructure have been considered targets, emphasis was on defense against a military threat. The Global War On Terror (GWOT) has created a number of heretofore unconsidered vulnerabilities in this traditional outlook. Many targets that would not be considered legitimate (economic, symbolic, etc.) in a conventional war must now be considered in strategic defensive planning. In conducting these attacks the unimpeded use of the sea is a force multiplier for an enemy dedicated to striking a wide range of potential targets. Possible threats from the sea are wide-ranging and diverse, relying on a combination of asymmetric offensive tactics while exploiting the variety of the littoral.

This asymmetric nature of GWOT requires a multi-agency approach to devise effective command and control for modern port defense. The Coast Guard and Navy have made important strides in this area by devising experimental Joint Harbor Operations Centers (JHOCs) as a component of maritime anti-terrorist force protection. The expansion of this concept into multi-agency maritime homeland security is a logical next step in the evolving problem of port security and defense. This is made evident by

examining likely terrorist threats to ports and studying the lessons of the past that apply in this environment which can be used to expand the current command and control system to meet the new threat

New Threat Matrix: Ports as Targets

The GWOT threat to ports is a relatively new element in the spectrum of naval warfare. This is largely due to the evolving nature of the shipping industry and the nation's growing reliance on sea power. Historically, a nation's maritime strength has been measured by the size and capability of its merchant fleet and Navy; attacks against a nation's sea power meant the physical destruction of these ships. Ports, until quite recently, were composed of infrastructure that was relatively easy to replace or replicate, making them relatively low priority targets for an enemy dedicated to striking at maritime strength.

This has changed in the modern era of containerization and the increased size and technical nature of ships. In modern times ports have become centers of highly technical, well-integrated infrastructure designed for the rapid loading and unloading of cargo, an evolution that has become highly complex in the era of containerization. Commercially efficient, port cargo operations are also highly dependent on networked operations, making the disruption of the process far simpler for a potential attacker. Additionally, the complexity of this evolution, combined with the increasing size of seagoing merchant vessels (and warships), has greatly reduced the number of commercial ports available for use by global shipping. This has the duel effect of making major ports more important economically and strategically while simultaneously making them more attractive targets for offensive action.

The attractiveness of ports as targets for terrorists can be summarized as follows:

A. Economic Impact: An unprecedented amount of trade – both imports and exports – relies on shipment by sea. A successful attack on maritime infrastructure would affect this trade in far greater proportion than the actual damage. It is likely that an attack on one port would have a cascade effect on others as increased security measures are applied nationwide. The recent impact of the London bombings can be seen as illustrative of this effect; although there was no indication of additional terrorist activity, security measures were increased at transportation hubs worldwide. Increasing security alerts at a train station is one thing; closing a huge economic entity such as a port is quite another. Delay of shipping in loading and offloading cargo is one of the most costly elements of the shipping process. We must also consider the impact to the shipping industry itself. During the Persian Gulf re-flagging operations of the late 1980s, for example, analysis showed the greatest impact to the shipping of oil was not the damage to tankers inflicted by the warring Iraqis and Iranians (which was, in fact, minimal), but the increased insurance costs of operating in that area.[3] An attack on a U.S. port could have a similar, if not larger, effect.

B. High visibility/High Casualties: Ports are not isolated areas, but rather major centers of commerce, usually surrounded by large cities and economic centers. An attack on a port could be highly visible and potentially the scene of mass conflagration. As a result of urban development, most major ports are no longer confined to strictly industrial areas,

but rather have become well-developed centers of commerce and entertainment, surrounded by built up waterside areas dedicated to tourism and recreation. Many of these facilities are located next to volatile maritime infrastructure (fuel tanks, docks, etc.) that could create mass conflagration if attacked through large explosive force. Sympathetic detonation, fires, and other catastrophic effects would certainly create mass casualties.

C. Ease of attack: Commercial ports are not fortresses. The ocean itself presents a number of distinct advantages to a dedicated attacker, especially when employing maritime suicide terrorism or means to rapidly deliver large explosive force. Water is not only a tremendously efficient transport medium (allowing for rapid transit), but the large amount of legitimate commercial and recreational traffic in ports allows for an enemy to mask movements prior to an attack, making effective defense difficult.

Given the importance of ports to our economy and military power, the potential for creating mass casualties, and the ease by which an enemy can attack, a strong case can be made that ports will become a target for future terrorist attacks. If this is the case, we can apply the military planning process to meeting this threat. The first step in this process is looking for lessons learned that could be used in the current scenario: have we faced this threat before, and if so, what can we learn from the experience?

Cold War Model

Port defense is not a new concept, but during the later stages of the Cold War port defense theory underwent considerable revision. In the mid-1980s the "long war," or prolonged NATO/Warsaw Pact conventional war scenario came into vogue with NATO planners. In such a conflict re-supply of Europe would become a top priority. If Europe was to be re-supplied from the United States it was assumed that, given the noted strength of the Soviet submarine fleet, the historical "Battle of the Atlantic" scenario would repeat itself using modern technology. If this were the case it was assumed the coastline of the United States would be a logical target for attack; historically, the Nazi U-boat offensive against the coast during the Second World War was particularly effective, destroying over 400 ships in an almost completely undefended littoral, a lesson that would not be lost on Soviet planners.[4] But unlike the historic scenario where ships were subject to conventional torpedo attack, it was argued that the targets of Soviet offensive power would likely be ports due to the large array of unconventional weaponry that could effectively target port infrastructure (mines, special operations teams, etc.) and the impact that such an attack would have on the overseas war effort.[5]

Accordingly, an entirely new Coast Guard-Navy command structure was designed to meet the anticipated threat.[6] In 1984 the Coast Guard and Navy stood up the Maritime Defense Zone (MDZ), a combined USCG-USN command tasked with the maritime defense of the United States 200nm seaward. Ports, especially strategic out load ports, were given a high priority in defensive planning in recognition of the high tech infrastructure that was necessary to load-out mass military supplies. This was arguably the first time since the Second World War that the defense of ports became a significant part of the national maritime strategy. Reflecting this priority, a new command and control system was designed and implemented for tactical defense. Ports and outload

operations were placed under Navy-Coast Guard "Sub-Sector" constructs that effectively combined defensive operations between the Services by co-locating Coast Guard and Navy personnel in operations centers that would oversee all military operations (including load out operations and critical infrastructure protection) within the port during time of national emergency.

Since we once again face a threat from the sea, it would be tempting to simply implement a defensive structure similar to that used in the past. But there are key differences between then and now that make this problematic. In the Cold War defense model, risk was very much a matter of proportionality and the threat to critical maritime infrastructure was distinctly military. In considering the "worst case" scenario, planners envisioned enemy actions in the littoral focusing on submarine attack, offensive mining, and special operations attacks against critical military infrastructure—in other words, attacks "from" the sea by conventional military means. It was assumed that "terrorist" actions would be sponsored by the enemy state and, as part of the enemy strategy, would not be directed against targets with limited or no military significance.

These core assumptions aided the defense effort considerably. In the re-supply of Europe scenario, "risk" was by no means an equal proposition. Ports were rated in strategic priority based on the amount of support they provided military forces overseas, the ports with the highest priority receiving the lion's share of the defensive forces. This strategy worked on a "floating" scale and was subject to change based on the evolving scenario; when New York City, for example, had completed its out load operations the priority (and subsequent defensive forces) shifted to the next port, allowing for a strategically "phased" defense.[7] In other words, we only needed to be strong in areas that were important to the war effort overseas—and this defensive strength was transitory at best.

The difference between "then and now" is telling when we consider potential targets and the subsequent effort required for defense. In the "old days," a strictly civilian target such as the WTC would not have been considered a valid target in New York City. The major weapons out load point at Earle, NJ, however, was Priority One for infrastructure protection. Obviously this has changed; targets in GWOT can be anywhere or anything. Maritime infrastructure that would not be considered critical in a Cold War scenario now has the potential to be targeted as a means of obtaining an economic or psychological victory. In this "new" scenario with its plethora of non-military targets and the potential offensive power of the enemy, there are not enough defensive forces to go around. This requires that we consider force multipliers beyond simple assets to improve the viability of the defense.

This is not to say that the Cold War model is completely invalid, or that we cannot learn from the lessons of history. What worked in the MDZ era was the establishment of a construct that emphasized joint communications, multi-service planning, and, above all, a multi-agency approach to defense of the port and its infrastructure. Force multipliers that can be employed in the current scenario revolve around the collection and use of multi-agency intelligence in a similar command and control construct for the protection of critical maritime infrastructure. In the "old" model, military intelligence sufficed to deal with a specific military threat against known target areas, with a response that was distinctly military. The new threat requires that we expand this model to consider all agencies within the port vital for total protection.

New Defensive Strategies

Maritime law enforcement (and by extension, protection of maritime critical infrastructure) is traditionally a Coast Guard mission. This has obviously evolved considerably as a result of the events of 9/11. When examining current port command and control proposals, it is useful to examine this evolution and how previous relationships can be employed in current operations.

A. Pre-9/11 Port Operations: Prior to 9/11 the Coast Guard port and offshore tactical constructs were divided into two separate areas of responsibility based on the type of law enforcement being conducted. In major ports the traditional Captain of the Port (COTP) position was assigned to a respective Marine Safety Offices (MSOs) responsible for the regulatory functions, such as vessel inspection, environmental response, licensing, etc. COTPs were (and are) responsible for merchant vessels entering and leaving port, conducting vessel inspections for maritime safety, and coordinating incident response. Maritime law enforcement conducted by MSOs was distinctly regulatory in nature; many vessel inspectors and recreational boating safety personnel performed their duties unarmed. Operations of a more traditional law enforcement variety, such as counter-narcotics or fisheries enforcement, search and rescue, and other offshore operations were the responsibility of a "Group" that maintained command and control of subordinate "Stations" in the Area of Responsibility (AOR) assigned that Group.[8] While this description is admittedly overly simplistic, it would be fair to say that MSOs "owned" the ports and all responsibilities for large merchant vessel and container operations that traditionally required regulatory attention, while Groups focused offshore and conducted law enforcement operations dealing with smaller maritime traffic or search and rescue. Afloat operational assets (utility boats, patrol boats, and small cutters) were generally "owned" by the Groups and used offshore in traditional law enforcement, although there was limited cooperation with the MSO for close inshore operations that required these assets.[9] It is important to note that both MSO/COTP and Group organizations maintained extensive relationships with other agencies working within the port and their respective areas of responsibility.

While this relationship and division of responsibility made sense prior to 9/11, the new asymmetric threat altered the equation considerably, requiring a merging of traditional responsibilities across established lines of command. The expanded threat spectrum now reached directly into the ports. Pure regulation, although still important for security, no longer sufficed; a direct law enforcement response capability (traditionally the role of Groups) was now required in the ports. Tracking and intercept of large merchant vessels, traditionally an MSO function, took on a new meaning as these vessels represent a potential threat to the security of the United States. Subsequently, merchant vessel regulation focusing on maritime security was "pushed" far offshore with the establishment of a layered defense.[10] The new threat also affected other agencies with maritime security concerns. Ports with a high Navy interest (including ports with Navy bases, research facilities, critical infrastructure, and out load responsibilities) that traditionally had some degree of Navy security immediately implemented extensive anti-terrorist force protection (ATFP) procedures to prevent, among other things, a "USS COLE" style attack on potentially vulnerable warships. U.S. Customs immediately

implemented increased forms of container and cargo security measures that were completely lacking prior to 9/11. It is clear from these new multi-agency security requirements that the somewhat laissez-faire command system exercised in the ports prior to 9/11 would no longer suffice in light of the new threat.

B. Post 9/11 Reorganization: The Coast Guard's answer to the post 9/11 threat was a merging of responsibility under a newly designed "Sector" organization, an effective combination of responsibilities and assets that has sole responsibility for all Coast Guard missions in one geographic area.[11] Sectors represent a merging of traditional Group and MSO/COTP functions, a significant cultural shift to "one mission" from several within each port. This re-organization soon took on a multi-agency nature. As noted, Coast Guard commands traditionally have close ties to other agencies in the ports, including Customs, Immigration, commercial organizations, and local, state, and federal law enforcement. This was reflected in the design of the new Sector Command Centers (SCCs). Tailored to meet local requirements, most SCCs possess either electronic links to other agencies operating in the port or staff positions for representatives from agencies to work in direct liaison with Coast Guard personnel on a daily or continuous basis. There are currently 44 SCCs operating or nearing completion.

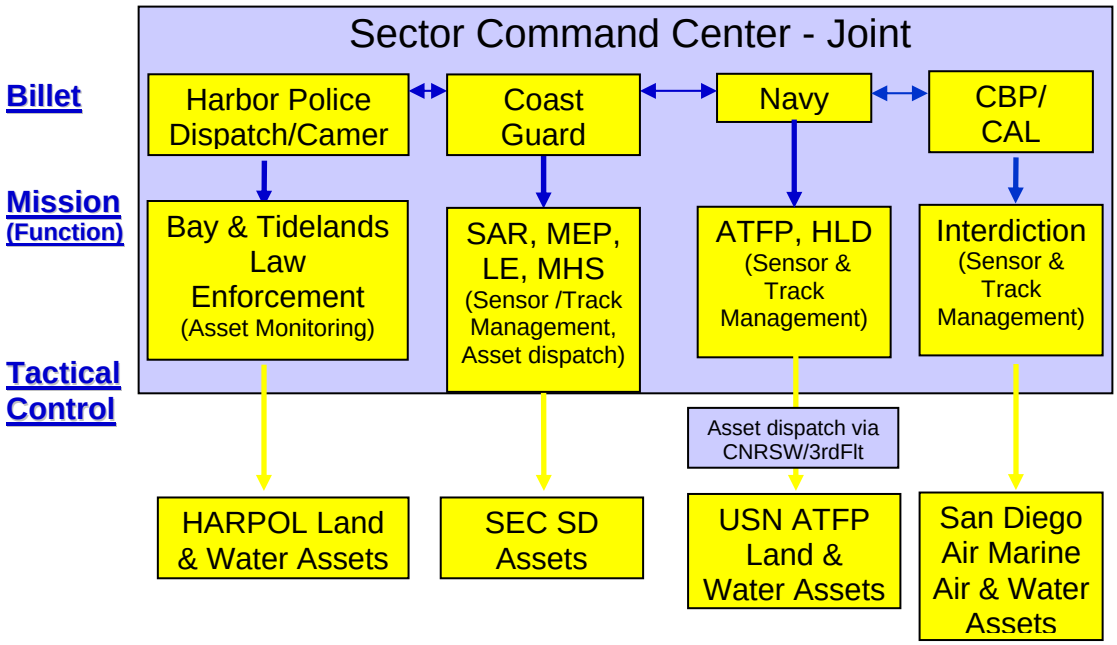
C. JHOCs: SCCs perform traditional port security and regulatory functions, but do not generally coordinate with DOD. In terms of critical maritime infrastructure protection this can be problematic, as much of the infrastructure is located in ports with a DOD presence, or is considered essential to DOD, and will therefore potentially fall under the auspices of Homeland Defense. This was recognized early in the SCC design process; the solution was similar to that employed during the MDZ era and stressed multi-service cooperation. Building on established infrastructure, Coast Guard and Navy designed a specialized SCC called the Joint Harbor Operations Center (JHOC), an experimental fusion center that quickly demonstrated its utility in providing for tactical operations between the Services. Recognizing a mutually beneficial interest in coordinating operations, the first JHOCs focused on fusing Coast Guard and Navy operations in port protection and ATFP in ports where the Navy had a large fleet presence.[12] Given their multi-agency approach to port security and littoral operations, JHOCs are a natural choice for the implementation of tactical port operations for maritime critical infrastructure protection. As such they can serve as a model for future execution of this mission.

JHOCs are far more than a merging of CG traditional roles and responsibilities with USN security procedures. Rather, they represent an important model for the fusing of intelligence and coordination of all multi-agency operations necessary for maritime critical infrastructure protection. As we have seen, Coast Guard and Navy cooperation is neither new nor particularly unique. Since the earliest days of each organization, both have used similar equipment and procedures in order to effectively operate together during time of war. But despite overseas operations in GWOT, U.S. ports are not on a war footing; rather, commerce and port operations continue at the normal pace, albeit under increased security procedures. Recognizing the number of agencies that operate in ports and the vast information requirements for maritime security and infrastructure protection, an effort was made to make JHOCs truly inter-agency by providing linkage to these agencies, including the establishment of formal liaison positions and data sharing

protocol, effectively merging regulation, law enforcement, and anti-terrorist force protection data and procedures.

The first experimental JHOCs were constructed and successfully tested in San Diego and Norfolk, ports that represented high strategic interest due to major Navy presence and the volume of overseas commercial traffic. These JHOCs' multi-agency design was based on relationships the Coast Guard had previously established during its normal operations within each port. This experimental design is illustrated in Figure 1 below:[13]

Figure 1: JHOC Structure



JHOCs possess several unique capabilities that contribute significantly to port and critical infrastructure protection. As command and control centers for ports and their immediate vicinity, JHOCs have inherent surveillance capability that can be fused into one multi-agency common operating picture (COP). Using the San Diego JHOC as an example, these systems include:

- USCG Coastal Radar
- USN Port control/offshore radar system
- Automated Identification System processors
- San Diego port control camera system (civilian)
- Navy waterside security system
- Border patrol camera/thermal imagery system

The initial success of JHOC San Diego and Norfolk led to a joint Coast Guard-Navy study to expand the project to all ports of strategic interest, using a three-tiered approach. Ports with navy presence, high commercial infrastructure, and 'outload' capability (loading of wartime material and supplies critical for overseas efforts) were considered for JHOC installation.

The Next Step: JHOCs as an Element of MCIP

Although there are only two fully functional JHOCs today, their evolving construct serves as a model for a future development of multi-agency cooperation in maritime critical infrastructure protection. Given the importance of our ports to national strategy, MCIP is a critical vulnerability that must be addressed by both DHS and DOD in one coordinated effort. We must recognize that this mission goes beyond traditional port security operations or anti-terrorist force protection, and as such demands a command and control construct that can truly fuse the myriad of responsibilities and operations in ports.

Multi-agency JHOCs offer several advantages for merging effective port operations and critical infrastructure protection. This is evident in the areas of intelligence fusion, coordinated planning, and tactical command and control.

A. Tactical intelligence fusion

In the post-9/11 analysis one of the greatest weaknesses cited by the 9/11 Commission was a lack of intelligence fusion between respective government agencies. JHOCs are designed to address this weakness on the tactical level, serving as fusion centers that effectively merge the various intelligence databases of each respective agency participating in the JHOC. Currently, these databases include the Coast Guard's Maritime Information Safety and Law Enforcement system, the Automated Regional Justice Information System (Naval Criminal Investigative Service), and intelligence from the local Joint Terrorism Task Force.[14] As JHOCs expand to include other agencies, this fusion function can naturally expand to include additional databases. In addition to using established databases, JHOCs also use inter-agency sensors and local inter-agency liaison to collect, fuse, and disseminate information that is critical for achieving a multi-agency tactical picture. This increased multi-agency awareness provides for streamlined operations between all port agencies, while the use of multi-agency sensors and databases allows for a tremendously enhanced capability for surveillance and anomaly detection, a crucial element in maritime critical infrastructure protection.

B. Coordinated planning for MCIP

One of the great advantages of a JHOC is the joint personnel structure that allows for both rapid and long-term on-scene multi-agency cooperation. Although primarily staffed by Coast Guard personnel, billets are being established for personnel from all agencies that have responsibility in the port, representing a unique merger of personnel with regulatory, law enforcement, and military expertise.[15] This liaison system is fundamental to the success not only for coordination of operations, but also to reach an understanding of multi-agency procedures and practices and infrastructure that each agency allots priority for protection. This is critical for tactical multi-agency planning. Given the large

number of regulatory agencies operating in each port, there are a number of procedures specific to each agency that can impact other multi-agency operations. Customs container inspections, for example, are a critical part of vessel tracking and re-routing performed by the Coast Guard; FBI tracking of potential terrorist suspects is a key element of ATFP for the Navy and facilities security forces. This type of information and, perhaps more importantly, how these procedures are carried out, can be provided immediately by effective liaison that merges agency operations into one efficient cooperative effort.

C. Multi-agency Command and Control

Ultimately maritime critical infrastructure protection is about the tactical coordination of multi-agency assets conducting port security and defense operations. JHOCs are first and foremost operations centers, possessing considerable command and control capability that can be used by multi-agency assets. By acting as combined, multi-agency fusion centers, JHOCs provide a unique tactical picture that all users can employ at the port level. Through its command and control apparatus, it is possible to coordinate tactical actions not only in crisis, but also in day-to-day port operations and exercises meant to improve multi-agency coordination.

CONCLUSIONS

Access to the sea is vital for economic expansion and as a means to project national power. Ports are essential in maintaining this link. But ports are not fortresses; as open industrial and commercial centers, port infrastructure is particularly vulnerable to a dedicated enemy. An effective attack against critical maritime infrastructure has the potential to cause major economic disruption nationwide, create mass casualties, and limit or halt deployment of naval power. As such, ports are logical targets for terrorists bent on striking at vulnerabilities; the destruction of ports would have significant impact on our nation.

Lessons from the past indicate that the key to effective defense is tactical coordination through dedicated multi-agency command and control. During the Cold War, the Coast Guard-Navy model for command and control was to deal with a military threat from the sea, but this has changed with the new asymmetric threat of GWOT. The diversity of the threat against our ports and the number of regulatory agencies that oversee critical infrastructure requires an expanded comprehensive command and control system that fuses multi-agency intelligence, has understanding of multi-agency capabilities, and can provide direction to these forces in the field. The JHOC concept has proven to be effective in multi-agency intelligence fusion and coordinated tactical port operations essential for maritime critical infrastructure protection and should be considered a model for coordinated port defense.

[1] www.dhs.gov/dhspublic

[2] J.Z. Heck, "Port Security: Nation Faces Formidable Challenges in Making New Initiative Successful" (Washington D.C.: GAO Publication No. GAO-2-993T (United States General Accounting Office), 3.

[3] www.cato.org/pus/pas/pa090.html

[4] Michael Gannon, *Operation Drumbeat,* (New York: Harper and Row, 1990), xviii.

[5] R. B. Watts, "Coastal Defense: Now More than Ever," (Annapolis: U.S. Naval Institute *Proceedings*, Dec. 1990), 66.

[6] Author's experience as an MDZ planner, 1988.

[7] The composition of Groups varies considerably. Traditionally, Groups are composed of a command center and have direct control of a number of smaller afloat assets, such as patrol boats and buoy tenders, and occasionally were co-located with air stations and controlled the helicopters/planes assigned to that station. "Stations" are smaller CG commands that maintain small offshore utility boats for near coastal SAR and law enforcement. Author's operational experience. See also P.J. Capelotti, "The Coast Guard's Response to 9/11," *Joint Center for Operational Analysis and Lessons Learned,* 4, Issue 4, September 2004.

[8] Each Group/MSO had individual Standard Operating Procedures (SOPs) that detailed this relationship, which varied in individual ports. The characterization/summary of these relationships is based on the author's operational experience.

[9] *Maritime Strategy for Homeland Security* (Washington D.C: U.S. Coast Guard, July 2002)

[10] Where applicable, Sector organizations also include Vessel Traffic Services (VTS) and CG Air Stations.

[11] It is important to note that at the time of this writing DOD participation in JHOCs are limited to ATFP, so USN presence in JHOCs are currently limited to areas of fleet or asset concentration. R. Watts, "JHOC Working Group Meeting/Briefing to Maritime Security Integration Group," 22 June 2005.

[12] "Pacific Area Capabilities and Interoperability for Homeland Security/Homeland Defense," Alameda: Unclassified briefing to Honorable Paul McHale, December 14" 2004.

[14] MSIG brief, 28 Feb 2004.

[15] Coast Guard Pacific Area (PACAREA) JHOC brief to author, December 2003